Patent Claims

1. A process for establishing a common cryptographic key for n subscribers using the DH process, characterized in that
- each of the n subscribers (I) is assigned one leaf of a binary-structured tree which has precisely n leaves and is of depth $\lceil \log_2 n \rceil$;
- for each subscriber (I), a secret (i) is generated and assigned to that leaf of the tree to which the respective subscriber (I) is also assigned;
- secrets are established consecutively in the direction of the tree root for all nodes (K) of the tree, where, starting from the leaves according to the defined tree structure across the entire hierarchy of the tree structure, two already known secrets are always combined via the DH process to form a new common secret and are allocated to a common node (K), so that the last node K_w and therefore the tree root contains the common key of all n subscribers as the secret.

2. The process as recited in Claim 1, characterized in that
- when a new subscriber is added to an existing tree structure which already has a common secret, in order to establish a common key for n+1 subscribers, two new leaves (B1 and B2) are added as successors to a leaf (B) at a suitable location of the binary tree, so that the new tree has precisely n+1 leaves and is of depth $\lceil \log_2 (n+1) \rceil$;
- the subscriber assigned to the previous leaf (B) and the new subscriber are each assigned to one of the new leaves (B1;B2), the previous leaf B becoming a common node for the new leaves (B1;B2);
- starting from the new leaves (B1;B2) and going as far as the root of the tree, new secrets are established only in those nodes which lie within the framework of the tree

structure on the path from leaves B1 and B2 to the tree root.

3. The process as recited in Claim 1,
characterized in that
- when a subscriber (B) is excluded from an already existing tree structure which already has a secret, both the leaf of the subscriber (B) to be removed as well as the leaf of the subscriber (A) assigned to the same common node are removed;
- the common node becomes the leaf of the subscriber A who is not to be removed, and starting from the leaves of the tree and going as far as the root, new secrets are established only in those nodes which lie within the framework of the tree structure on the path from the new leaf (A) to the tree root.

Add
A1